

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-215242

(43)Date of publication of application : 11.08.1998

(51)Int.Cl.

H04L 9/08
 G06F 15/00
 G06F 17/60
 G09C 1/00
 H04L 9/14
 // G06F 12/14

(21)Application number : 09-016085

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 30.01.1997

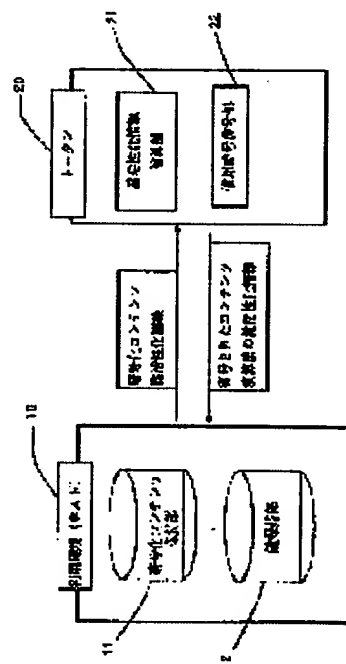
(72)Inventor : KIKO KENICHIROU
 SAITO KAZUO

(54) AUTHENTICATION METHOD AND DEVICE THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To execute the control of utilization sequence of enciphered contents in off-line.

SOLUTION: In the case of using a first key, a corresponding key is retrieved from a key storage section 12 based on an ID imparted to contents. A value of a field denoting a remaining number of times corresponding to the key in the key storage section 12 and when the value is zero, a host 10 sends the contents and the key to a token 20. A decoding section 22 of the token 20 uses the key to decode the contents and sends the result to the host 10. The host 10 checks an ID of a key used next to the present key from the key storage section 12. When the ID of the next key is not zero, the host 10 retrieves the next key based on the ID and conducts key activation processing when the corresponding key is found out. When the ID of the next key is zero, since the next key is not in existence, no key activation processing is conducted. The host 10 utilizes the decoded contents.



LEGAL STATUS

[Date of request for examination] 04.07.2001
 [Date of sending the examiner's decision of rejection] 14.12.2004
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection] 2005-00690
 [Date of requesting appeal against examiner's decision of rejection] 12.01.2005
 [Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-215242

(43) 公開日 平成10年(1998) 8月11日

(51) Int.Cl. ⁸	識別記号	F I	
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z
	17/60	G 0 9 C 1/00	6 6 0 B
G 0 9 C 1/00	6 6 0	G 0 6 F 12/14	3 2 0 B
H 0 4 L 9/14		15/21	Z

審査請求 未請求 請求項の数15 O L (全 22 頁) 最終頁に続く

(21) 出願番号 特願平9-16085

(22) 出願日 平成9年(1997) 1月30日

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 木子 健一郎

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

(72) 発明者 齊藤 和雄

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

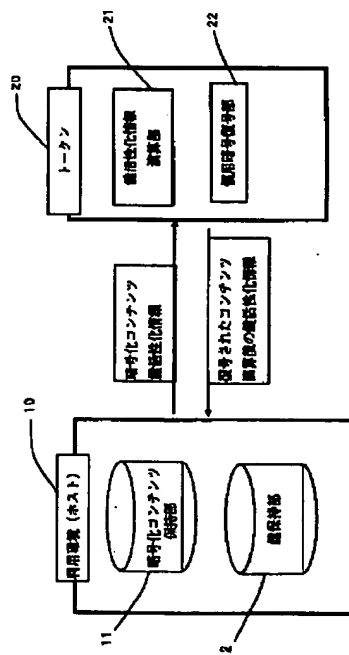
(74) 代理人 弁理士 澤田 俊夫

(54) 【発明の名称】 認証方法および装置

(57) 【要約】

【課題】 暗号化されたコンテンツの利用順序の制御をオフラインで実施できるようにする。

【解決手段】 最初の鍵を使用する際にはコンテンツに付与されたIDを基に対応する鍵を、鍵保持部12より検索する。鍵保持部12の鍵に対応する残り回数のフィールドの値を調べ、値が0の場合にはホスト10はトークン20にコンテンツと鍵を送る。トークン20の復号部22は鍵を利用してコンテンツを復号しホスト10に送る。ホスト10は、鍵保持部12から、現在の鍵の次に使用できる鍵のIDを調べる。次の鍵のIDが0でない場合、IDをもとに次の鍵を検索し、対応する鍵が見つかった場合には、鍵活性化処理を行う。次の鍵のIDが0の場合には、次の鍵は存在しないので、鍵活性化処理は行わない。ホスト10は、復号されたコンテンツを利用する。



【特許請求の範囲】

【請求項1】 異なる認証を所定の順序で行う認証方法において、

先順序の認証のために対応する先順序の証明情報を利用するステップと、

上記先順序の証明情報の利用に基づいて、後順序の認証のための後順序の証明情報を生成するステップと、

上記後順序の認証のために上記後順序の証明情報を利用するステップとを有することを特徴とする認証方法。

【請求項2】 順序付けて生成された、特定のユーザに対する特定の権利を証明するための証明情報の系列を利用して上記証明情報に対応した認証を行う認証方法において、利用されるべき順序が先である証明情報を利用する際に、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を、生成された証明情報活性化情報に基づいて活性化することによって、証明情報の系列を予め決められた順序でのみ利用できることにしたことを特徴とする認証方法。

【請求項3】 複数の証明情報から生成された複数の証明情報活性化情報をもとに特定の演算を施す事により、他の証明情報を活性化するための活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行う請求項2記載の認証方法。

【請求項4】 証明情報を利用することで生成される活性化情報を保持しておき、次に同じ証明情報を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く証明情報を活性化することができる証明情報活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行う請求項2記載の認証方法。

【請求項5】 順序付けられた、特定のユーザに対する特定の権利を証明するための証明情報の系列を生成する証明情報生成方法において、利用されるべき順序が先である証明情報から、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を証明情報活性化情報に基づいて改変して生成することによって、先の証明情報を使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしたことを特徴とする証明情報生成方法。

【請求項6】 複数の証明情報から証明情報を活性化するための証明情報活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の証明情報を改変して生成することによって、複数の証明情報を使用することによって、改変した証明情報を有効にするための証明情報活性化情報が得られるようにした請求項5記載の証明情報生成方法。

【請求項7】 利用されるべき順序が先である証明情報から、それに続く証明情報を生成する際に、順序が先で

ある鍵が持つ証明情報活性化情報の初期値に対して複数回の定められた演算を施す事により生成される証明情報活性化情報に基づいて、それに続く証明情報を改変して生成することによって、先の証明情報を複数回使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにした請求項5記載の証明情報生成方法。

【請求項8】 特定のユーザが特定の権利を有することを証明するための証明情報によって、ユーザが正当な権利者であることを認証する装置であって、証明情報を処理して認証を行う際に、それと同時に、当該証明情報に後続して使用されるべき証明情報を使用可能とするための認証情報活性化情報の基となる情報から、後続する証明情報の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する証明情報を利用可能とする証明情報活性化手段を有することを特徴とするユーザ認証装置。

【請求項9】 一連の順序付けられた暗号鍵系列の利用を制御する暗号鍵順序制御方法において、利用されるべき順序が先である鍵を利用する際に、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を、生成された暗号鍵活性化情報に基づいて活性化することによって、暗号鍵系列を予め決められた順序でのみ利用できることにすることを特徴とする暗号鍵利用順序制御方法。

【請求項10】 複数の鍵から生成された複数の活性化情報をもとに特定の演算を施す事により、他の暗号鍵を活性化するための活性化情報が生成される請求項9記載の暗号鍵利用順序制御方法。

【請求項11】 暗号鍵を利用することで生成される活性化情報を保持しておき、次に同じ暗号鍵を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く暗号鍵を活性化するための暗号鍵活性化情報が生成される請求項9記載の暗号鍵利用順序制御方法。

【請求項12】 一連の順序付けられた暗号鍵系列を生成する暗号鍵生成方法において、利用されるべき順序が先である鍵から、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を暗号鍵活性化情報に基づいて改変して生成することによって、先の鍵を使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしたことを特徴とする暗号鍵生成方法。

【請求項13】 複数の鍵から暗号鍵を活性化するための暗号鍵活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の暗号鍵を改変して生成することによって、複数の鍵を使用することによって、改変した鍵を有効にするための暗号鍵活性化情報が得られるようにした請求項

12記載の暗号鍵生成方法。

【請求項14】 利用されるべき順序が先である鍵から、それに続く暗号鍵を生成する際に、順序が先である鍵が持つ暗号鍵活性化情報の初期値に対して複数回の定められた演算を施す事により生成される暗号鍵活性化情報に基づいて、それに続く鍵を改変して生成することによって、先の鍵を複数回使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにした請求項12記載の暗号鍵生成方法。

【請求項15】 暗号化されたデジタル情報を復号して利用するための復号装置であって、復号鍵によって当該暗号化データを復号する際に、それと同時に、当該復号鍵に後続して使用すべき復号鍵を使用可能とするための復号鍵活性化情報の基となる情報を入力として、後続復号鍵の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する復号鍵を利用可能とする復号鍵活性化手段を有することを特徴とした復号装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数の認証を所定の順序で行う認証技術に関し、その順序を逸脱した場合には認証が正しく行われなくないようにしたものである。また本発明は、先の順序の証明情報を利用することにより暗号化されたデジタル情報を復号して利用する場合の、暗号鍵の生成方法に関し、あらかじめ定められた順序に従ってデジタル情報を特定の回数利用することにより、次に定められた暗号鍵が生成される技術に関する。

【0002】なお、本発明の利用範囲はコンテンツを暗号化して流通させ、その利用順序を制御するだけにとどまらず、一般に暗号鍵（署名のための鍵、検証のための鍵など、暗号技術における鍵、一般）の利用順序の制御を可能とするものである。

【0003】従って例えば、電車の乗車券や映画の鑑賞券のようなチケットを電子的に発行する場合に、乗車券はキセルを防ぐために予め決められた順序でしか乗車券を使えないようにしたり、あるいはある映画を見ると別の映画を安く見ることができるなどの鑑賞券の売り方を実現する際にも、電子的に発行されたチケットの利用順序の制御にも適用することが可能である。

【0004】

【従来技術】近年のネットワークの発達により様々な情報がデジタル化され、流通するようになってきている。デジタル情報は複写が容易であり、複写されたものは劣化しないという特質があるため、金銭的な価値を持つデジタルコンテンツ（画像、動画、プログラムなど）を暗号化して流通させ、使用時にユーザの環境で復号して利用するという流通形態が開始され始めている。NTT社のmiTaKaTTa（商標）や、IBM社のInfo market（商標）が現在実施されている代表的なサ

ービスである。コンテンツが共通の鍵で暗号化されて配布される場合には、一旦鍵が露呈するとその鍵が流布することによってコンテンツがただで利用されてしまうという問題がある。そこで、これらのサービスではコンテンツを利用する時のみ、オンラインで一時的に鍵を配布し、利用が終わると鍵は捨てられるように構成されている。

【0005】しかし、この構成ではコンテンツの利用がオンラインでしかできないことになり、ユーザに対して通信コストの負担不便を強いることになる。

【0006】一方、それに対して特公平6-95302号公報のソフトウェア管理方式や、Wave System社の開発したWave Chip（商標）などの技術では、コンテンツは予め決められた暗号鍵で暗号化されて流通させ、利用者はそれを復号するための共通の鍵の封入されたICカードあるいはICチップを自分のPCに接続し、利用したいときはその装置内で復号してコンテンツを利用するというような形態により構成している。ICカードなどのデバイス内では利用することに履歴が取られ、後でその履歴に応じて料金を徴収するというものであった。

【0007】しかし、この方法によるとユーザの資格などに応じて、利用可能なコンテンツを制限したりすることは不可能であった。

【0008】そこで、本出願人はあらたなユーザ認証技術を提案している（特願平9-418号）。この提案によれば、コンテンツは共通の鍵で暗号化し、ユーザは自分自身の鍵を持ち、アクセスチケットと呼ぶコンテンツとユーザの間を取り持つためのチケットを導入することで、暗号化されたコンテンツのオフラインでの利用を可能とし、さらにユーザ毎にアクセスチケットの発行をコントロールして、アクセス制限を行うことを可能としている。

【0009】

【発明が解決しようとする課題】しかしながら、特願平9-418号の提案によると、コンテンツを利用するためのアクセスチケットはそれを発行可能であるコンテンツの配布者あるいはチケット発行センターのような機関に依頼せねばならない（以下、簡単のためこれらを総称してセンターと呼ぶ）。すなわち、ユーザはアクセスチケットを一旦手に入れてしまえばオフラインで使い続けることが可能となるが、新たなコンテンツを利用しようとした場合には前記センターにオンライン（あるいはそれに代わる手段）で依頼しなければならないことになる。

【0010】予め幾つかの部分に分割され、それらが順序だてて利用されることを想定して作られたコンテンツ、例えば小説や物語、段階を追って難しくすることを意図した問題集などでは、これらのコンテンツは部分に分割され、それぞれの部分ごとに異なった暗号化が施さ

れ、それぞれ利用する際には異なるアクセスチケットを要求するように構成される。

【0011】しかし、コンテンツの利用順序を限定しようとするためには、センターはユーザに対して一括してアクセスチケットを発行することはできないため、ユーザは新たな部分を利用したいと思う度にアクセスチケットを手に入れるためにセンターに発行を依頼しなければならないことになる。

【0012】また、利用順序が線形でなく、二つの異なったコンテンツを順序に関わりなく利用することにより、別のコンテンツが利用可能になるという、提供方法もある。このような販売形態を採ろうとすると、従来の方法では、やはりユーザは三つ目のコンテンツを利用するためのチケットをセンターに発行依頼しなければならない。

【0013】

【発明が解決しようとする課題】本発明は上記のような問題に鑑みてなされたものであり、その目的とするところは、ユーザによる暗号化されたコンテンツ（あるいは暗号鍵）の利用順序の制御をオフラインで実施可能であるようにすることにある。

【0014】

【課題を解決するための手段】まず、本発明の概要について具体的な実現環境に即して説明する。本発明の1実現環境では、上記の課題を解決するため、ユーザ環境をコンテンツの利用環境と、あらかじめユーザ毎に配られるトークンによって構成する。トークンはICカードなどの演算機能を持つ耐タンパー容器である。そして、ある鍵に対して特定の演算を複数回繰り返す事で、始めて次に指定された鍵が生成されるように計算された複数の鍵を発行し、ユーザ環境においてトークンがこの定められた演算を行った結果を基にして、次の鍵を生成することで次の鍵が利用可能になる。

【0015】また、本発明は上記の課題を解決するため、アクセスチケットを用いたアクセス制御方法（特願平9-418号）において、一連の複数のチケットとそれぞれのチケットに対応する利用制限情報をあらかじめ決められた計算方法に基づいて発行する。アクセスチケットの利用制限情報には、このチケットの使用順位もしくは次に使用するチケットを識別する数値、次のチケットを使用可能にするためのチケット活性化情報、次のチケットが使用可能になるまでの回数、及び次のチケットの法数のフィールドが含まれる。そして、発行した複数のチケットと、最初に用いるチケットに対応する利用制限情報のみをユーザに配布する。

【0016】あるチケットの次のチケットを使用可能にするためのチケット活性化情報は、現在使用しているチケットを用いて、トークンとの間で定められた回数の通信を行う事でのみ生成される。こうして生成されたチケット活性化情報を、次に使用するチケットの利用制限情

報の特定のフィールドに追加する事により、はじめて次のチケットが使用可能になる。

【0017】次のチケットは異なるコンテンツに対するものであってもよいし、同一のコンテンツに対して、異なる利用条件での使用を許可するものであってもよい。

【0018】さらに、本発明の構成について詳細に説明する。

【0019】本発明によれば、上述の目的を達成するために、異なる認証を所定の順序で行う認証方法において、先順序の認証のために対応する先順序の証明情報を利用するステップと、上記先順序の証明情報の利用に基づいて、後順序の認証のための後順序の証明情報を生成するステップと、上記後順序の認証のために上記後順序の証明情報を利用するステップとを実行するようにしている。

【0020】この構成においては、先順序の証明情報を実際に使用して初めて後順序の証明情報が利用可能になり、認証を所定の順番で行うように強制できる。

【0021】また、本発明によれば、上述の目的を達成するために、順序付けて生成された、特定のユーザに対する特定の権利を証明するための証明情報の系列の利用して上記証明情報に対応した認証を行う認証法補において、利用されるべき順序が先である証明情報を利用する際に、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を、生成された証明情報活性化情報に基づいて活性化することによって、証明情報の系列を予め決められた順序でのみ利用できるようにしている。

【0022】この構成においては、先の証明情報が利用されて、後の証明情報が活性化されるので、証明情報の系列を予め決められた順序でのみ利用するように強制できる。

【0023】また、この構成において、複数の証明情報から生成された複数の証明情報活性化情報をもとに特定の演算を施す事により、他の証明情報を活性化するための活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行うようにしてもよい。

【0024】また、証明情報を利用することで生成される活性化情報を保持しておき、次に同じ証明情報を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く証明情報を活性化することができる証明情報活性化情報が生成され、生成された活性化情報によって活性化された証明情報を用いて認証を行うようにしてもよい。

【0025】また、本発明によれば、上述の目的を達成するために、順序付けられた、特定のユーザに対する特定の権利を証明するための証明情報の系列を生成する証明情報生成方法において、利用されるべき順序が先であ

る証明情報から、それに続く証明情報を活性化するための証明情報活性化情報を生成し、それに続く証明情報を証明情報活性化情報に基づいて改変して生成することによって、先の証明情報を使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしている。

【0026】この構成においても、先の証明情報が利用されて、後の証明情報が生成されるので、証明情報の系列を予め定められた順序でのみ利用するように強制できる。

【0027】また、この構成において、複数の証明情報から証明情報を活性化するための証明情報活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の証明情報を改変して生成することによって、複数の証明情報を使用することによって、改変した証明情報を有効にするための証明情報活性化情報が得られるようにしてもよい。

【0028】また、利用されるべき順序が先である証明情報から、それに続く証明情報を生成する際に、順序が先である鍵が持つ証明情報活性化情報の初期値に対して複数回の定められた演算を施す事により生成される証明情報活性化情報に基づいて、それに続く証明情報を改変して生成することによって、先の証明情報を複数回使用することによって、はじめて後の証明情報を有効にするための証明情報活性化情報が得られるようにしてもよい。

【0029】また、本発明によれば、上述の目的を達成するために、特定のユーザが特定の権利を有することを証明するための証明情報によって、ユーザが正当な権利者であることを認証する装置において、証明情報を処理して認証を行う際に、それと同時に、当該証明情報に後続して使用されるべき証明情報を使用可能とするための認証情報活性化情報の基となる情報から、後続する証明情報の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する証明情報を利用可能とする証明情報活性化手段とを設けるようにしている。

【0030】この構成においても、先の証明情報が利用されて後の証明情報が活性化されるので、証明情報の系列を予め定められた順序でのみ利用するように強制できる。

【0031】また、本発明によれば、上述の目的を達成するために、一連の順序付けられた暗号鍵系列の利用を制御する暗号鍵順序制御方法において、利用されるべき順序が先である鍵を利用する際に、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を、生成された暗号鍵活性化情報に基づいて活性化することによって、暗号鍵系列を予め決められた順序でのみ利用できるようにしている。

【0032】この構成においては、複数の鍵から生成さ

れた複数の活性化情報をもとに特定の演算を施す事により、他の暗号鍵を活性化するための活性化情報が生成されるようにしてもよい。

【0033】また、暗号鍵を利用することで生成される活性化情報を保持しておき、次に同じ暗号鍵を利用するときには、前回生成された活性化情報に対してさらに活性化のための演算を行い、この操作を定められた回数繰り返す事により、はじめてそれに続く暗号鍵を活性化するための暗号鍵活性化情報が生成されるようにしてもよい。

【0034】また、本発明によれば、上述の目的を達成するために、一連の順序付けられた暗号鍵系列を生成する暗号鍵生成方法において、利用されるべき順序が先である鍵から、それに続く暗号鍵を活性化するための暗号鍵活性化情報を生成し、それに続く鍵を暗号鍵活性化情報に基づいて改変して生成することによって、先の鍵を使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしている。

【0035】この構成においては、複数の鍵から暗号鍵を活性化するための暗号鍵活性化情報をそれぞれ生成し、それらの複数の活性化情報に特定の演算を施した結果に基づいて、それらとは別の暗号鍵を改変して生成することによって、複数の鍵を使用することによって、改変した鍵を有効にするための暗号鍵活性化情報が得られるようにしてもよい。また、利用されるべき順序が先である鍵から、それに続く暗号鍵を生成する際に、順序が先である鍵が持つ暗号鍵活性化情報の初期値に対して複数回の定められた演算を施す事により生成される暗号鍵活性化情報に基づいて、それに続く鍵を改変して生成することによって、先の鍵を複数回使用することによって、はじめて後の鍵を有効にするための暗号鍵活性化情報が得られるようにしてもよい。

【0036】また、本発明によれば、上述の目的を達成するために、暗号化されたデジタル情報を復号して利用するための復号装置に、復号鍵によって、当該暗号化データを復号する際に、それと同時に、当該復号鍵に後続して使用すべき復号鍵を使用可能とするための復号鍵活性化情報の基となる情報を入力として、後続復号鍵の活性化情報を計算する活性化情報計算手段と、それによって得られた活性化情報によって、後続する復号鍵を利用可能とする復号鍵活性化手段とを設けるようにしている。

【0037】この構成においては、先行する復号鍵を利用することにより後続の復号鍵を活性化させることで可能となり、予め定められた順序で復号を行うことが可能となる。

【0038】

【発明の実施の態様】以下、本発明の実施例について説明する。

【0039】〔実施例1〕本実施例では、1つの暗号化

10

20

30

40

50

鍵を特定の回数用いる事により、異なるコンテンツに対する暗号化鍵を生成する方法について述べる。

【0040】本実施例は、デジタルコンテンツを暗号化して鍵と共に提供するコンテンツプロバイダと、提供されたコンテンツを復号して利用するためのユーザ環境とからなる。

【0041】図1は、ユーザ環境を示しており、この図において、ユーザ環境は、利用環境（ホスト）10とトークン20とからなり、利用環境10は暗号化されたデジタルコンテンツを保持するコンテンツ保持部11と、それに対応する鍵を保持する鍵保持部12とを含んで構成されている。トークン20はあらかじめユーザ毎に配布される、スマートカードやICカードであり、鍵を活性化させるための演算部21とコンテンツ、もしくはコンテンツを復号するための情報を復号するための復号部22を持つ。

【0042】次に実施例の動作について図2および図3を参照して述べる。図2は実施例の全体的な処理を示す。図3は鍵活性化処理の詳細を示す。

【0043】なお、本実施例では、コンテンツプロバイダは4つの異なるコンテンツが順番に利用されるように、鍵を発行する。始めにコンテンツプロバイダは、コンテンツを慣用暗号鍵K1で暗号化する。さらに、他のコンテンツを、利用する順番にそれぞれK2～K4の鍵で暗号化する。そして、以下のように、K2'～K4'を計算する。

【0044】

【数1】 $K2' = K2 - F^{Ur2} (K1)$

$K3' = K3 - F^{Ur3} (K2)$

$K4' = K4 - F^{Ur4} (K3)$

$F^{Ur2} (K1)$ はK1に対してFの演算をUr2回繰り返す事を意味している。

【0045】Fは一方方向性関数（例えばMD5などのハッシュ関数）、Urは次のチケットを使用可能にするために現在のチケットを使用しなければならない回数である。Fの計算方法を秘密とし、ユーザ毎にその計算方法を異なるものとすれば、他のユーザが計算した値を流用される事はない。ユーザには、K1とK2'～K4'および、Ur2～Ur4が配布される。ユーザに配布された鍵は鍵保持部12に保持される。一連の鍵が配布された時点での、鍵保持部12の様子を図4に示す。

【0046】さて、図2において、最初の鍵を使用する際にはコンテンツに付与されたIDを基に対応する鍵を、鍵保持部12より検索する（S10）。対応する鍵が無い場合は処理を終了する（S11）。次に、鍵保持部12の鍵に対応する残り回数のフィールドの値を調べ、値が0でない場合はその鍵はまだ有効ではないので、やはり処理を終了する（S12）。ホスト10はトークン20にコンテンツと鍵を送る（S13）。トークン20の復号部22は鍵を利用してコンテンツを復号し

ホスト10に送る（S14）。ホスト10は、鍵保持部12から、現在の鍵の次に使用できる鍵のIDを調べる（S15）。次の鍵のIDが0でない場合、IDをもとに次の鍵を検索し、対応する鍵が見つかった場合には、鍵活性化処理を行う（S16～S19）。次の鍵のIDが0の場合には、次の鍵は存在しないので、ホスト10は復号されたコンテンツを利用する（S20）。

【0047】次に図3を参照して鍵活性化処理S19について詳細に述べる。図3において、鍵活性化処理では、まず鍵保持部12から鍵に対応する鍵活性化情報を取得する（S21）。この値が0であった場合には、鍵活性化情報のフィールドに、現在の鍵の値を書き込む（S22、S23）。次に、ホスト10はトークン20に現在の鍵活性化情報αを送る（S24）。トークン20は $F(\alpha)$ を計算しホスト10にその値を返す（S25）。鍵保持部12の、次の鍵の残り回数Urの値（図4）を1減らす（S26）。1減らした結果、残り回数Urの値が0にならない場合には、ユーザ環境は $F(\alpha)$ の値で、現在の鍵の活性化情報を置き換える（S27、S28）。値が0になった場合には、次の鍵の値に $F(\alpha)$ を足したもので、次の鍵の値を置き換える（S29）。このようにして2番目の鍵が使用可能になった時点での、鍵保持部の様子を図5に示す。これで、鍵活性化処理は終了し、ホスト10は復号されたコンテンツを利用する。

【0048】このように一連の鍵を上記のような方法で、関連付けて作成する事により、第一の鍵K1を特定回数使うことにより、初めて、第二の鍵K2を計算する事ができ、これにより第二の鍵K2が利用可能になる。同様の処理により、順次異なる鍵を、定まった順序・回数でのみ利用する仕組みが実現できる。

【0049】〔実施例2〕本実施例では、特に1つのコンテンツを特定の回数用いる事により、異なる利用条件での使用を可能にする方法について述べる。例えば、あるコンテンツを特定回数用いることで、より安い料金での使用を可能にするような方法である。

【0050】また、本実施例は、本発明を特願平9-418号のユーザ認証技術に適用した例である。

【0051】はじめに、本実施例で用いられるアクセスチケット（認証用補助情報）を用いた処理の概観を説明する。図6に処理の概観を示す。図6において、アクセスチケットを用いた処理は、チケット発行センタ30と、コンテンツプロバイダ40、及びユーザ環境50から構成されるシステムにおいて実行される。

【0052】チケット発行センタ30は、チケット公開鍵データベース31、ユーザデータベース32、プロバイダデータベース33及びアクセスチケット発行装置34を持つ。コンテンツプロバイダ40は、暗号化していないコンテンツと、慣用暗号鍵を保持し、慣用暗号装置よりコンテンツを暗号化する。

【0053】また、ユーザ環境50は、パソコンやワークステーションなど、デジタル情報を利用するための情報処理装置である利用環境（ホスト）51と、利用者の認証をするためにホスト51に接続されているトークン52とを含んでなる。ホスト51はユーザツール53およびカプセル化コンテンツ54を含む。トークン52は、各利用者に固有の情報を安全に封入したICカードもしくはスマートカードのような耐タンパー容器であり、固有情報をもとに利用者の認証を行うための演算部を有している。トークン52はあらかじめ各利用者に配布されている。

【0054】はじめに、コンテンツプロバイダ40は、コンテンツを暗号化する慣用暗号鍵を暗号化するために必要なRSA（Rivest, Shamir, Adleman）公開鍵の発行を、チケット発行センタ30に対して要求する(①)。チケット発行センタ30は要求に応じて、公開鍵をコンテンツプロバイダ40に送付する(②)。コンテンツプロバイダ40は自身で用意した慣用暗号鍵でコンテンツを暗号化し、その鍵をさらに発行された公開鍵で暗号化してコンテンツ内に特定の方法で埋め込む。こうして出来上がったコンテンツ（カプセル化コンテンツ）が、利用者（ユーザ環境）50にネットワークやCD-ROMなどを用いて配布される(③)。コンテンツは暗号化されているため、このままでは利用する事ができない。利用者は利用したいコンテンツ及び自分のユーザIDに対応したアクセスチケットの発行をセンタ30に要求する(④)。アクセスチケットは、特定のコンテンツとユーザの固有情報がそろったときのみ、そのコンテンツを利用可能にするためのデジタル情報であり、他のユーザとコンテンツの組み合わせでは使用できない。センタ30はユーザの要求に応じてアクセスチケットを発行しユーザに送付する(⑤)。ユーザはアクセスチケットを用いてコンテンツを利用する。アクセスチケットにはアクセス制御のための情報以外に、利用料金や支払方法、使用期限などの利用条件に関する情報が付与されている。ユーザがコンテンツを利用すると、利用に応じてその履歴がトークン52に記録される。この際、履歴にはその利用時点での利用条件も同時に記録される。ユーザは適当なタイミングで、センタ30に利用履歴を送付する(⑥)。センタ30は回収した利用履歴に基づいて課金を行う。回収した履歴に基づいて計算された料金が、それぞれの利用者の口座より引き落とされ、コンテンツプロバイダ40に各コンテンツの利用量に応じて分配される(⑦)。

【0055】次に、本実施例での処理を詳しく説明する。

【0056】はじめに、コンテンツプロバイダ40は、コンテンツを暗号化する慣用暗号鍵を暗号化するために必要なRSA公開鍵ペアE、Dと法数nをセンタ30より発行してもらう。コンテンツプロバイダ40にはEと

nが渡され、センタ30は発行した公開鍵に対応する秘密鍵D、法数nを公開鍵データベース31に記録して安全に管理しておく。次に、コンテンツプロバイダ30は自身で用意した慣用暗号鍵Kによりこのコンテンツを暗号化する。さらに、このKをセンタより発行された公開鍵Eで暗号化し、 $K^* = K^E \bmod n$ を作成する。この K^* をコンテンツ内に特定の方法で埋め込む。こうして出来上がったコンテンツ（以下カプセル化コンテンツと呼ぶ）は、利用者にネットワークやCD-ROMなどを用いて配布される。

【0057】ユーザはコンテンツを利用するため、アクセスチケットの発行をセンタ30に依頼する。図7にアクセスチケットの構成を示す。アクセスチケットは認証情報（以下単にチケットと呼ぶ）tと、利用制限情報L、チケット法数n、及び公開鍵Eからなる。アクセスチケットとコンテンツは一意に対応しており、コンテンツの公開鍵法数nによって対応関係を決定することができる。

【0058】ここで、ある一定回数の利用後には異なった利用条件（例えば割引料金）での使用を可能にするため、アクセスチケットを発行する際に、センタ30は以下のように、複数のチケットとそれに対応する利用制限情報を用意する。本実施例では4種類の異なる利用条件を持つアクセスチケットとそれに対応する利用制限情報を用意する。

【0059】

【数2】 $t1 = D + F(du, L1, n)$

$t2 = D + F(du, L2, n)$

$t3 = D + F(du, L3, n)$

$t4 = D + F(du, L4, n)$

利用制限情報を図8に示す。

【0060】上記の式および図8において、式「 $(\alpha 1)^{Fur2(du, L1, n)} \bmod n$ 」は、 $\alpha 1$ を $F(du, L1, n)$ でUr2回べき乗し、nに関する剰余をとることを表す。tはチケット、Dはコンテンツの公開鍵に対応する秘密鍵、Fは一方方向性関数（例えばMD5などのハッシュ関数）、duはユーザの秘密鍵、nはコンテンツの公開鍵法数、Irはチケット発行時に生成される乱数、Lは利用条件などを記した利用制限情報である。

【0061】利用制限情報Lは、対応するチケットによるコンテンツの利用に関する情報を記述したもので、アクセスチケットが利用できる期限を示す使用期限や、このチケットによってコンテンツを利用した場合の1回の利用料金などが記述されている。コンテンツを利用した場合には、この情報に従って課金が行われる。さらに、利用制限情報Lには、このアクセスチケットの使用順位、次のアクセスチケットを使用可能にするためのチケット活性化情報 α 、及び次のアクセスチケットが使用可能になるまでの回数Urが含まれている。

【0062】チケット生成時には、 t は L を図8に示すように設定して計算される。すなわち、 U_r の値を全て0とし、 α の計算にのみ実際の U_r の値が用いられる。 n 、 D の値はセンタ30内の公開鍵データベース31を、 du の値はユーザデータベース32を参照する事により得ることができる。

【0063】ユーザには t_1 から t_4 の一連のチケットと、利用制限情報 $L_1 \sim L_4$ を含むアクセスチケットが配布される。但し、ユーザへの配布時には $L_1 \sim L_4$ は、図9に示すように $U_{r1} \sim U_{r4}$ に値が設定され、さらに $L_2 \sim L_4$ の $\alpha_2 \sim \alpha_4$ の値を0としたものに置き換えられる。

【0064】図10にユーザ環境50（図6）の構成を示す。ユーザ環境50は利用環境（ホスト）51とトークン52からなり、トークン52は証明情報演算部64およびユーザ固有情報保持部65を有している。ユーザ固有情報保持部65には各ユーザに固有の情報が入れられている。固有情報はユーザには秘密であり、ユーザのIDとそれに対応する固有情報は、チケット発行センタ30で安全に管理されている。

【0065】利用環境（ホスト）51は、カプセル化コンテンツ54とユーザツール53とを有する。ユーザツール53は、アクセスチケット保持部（複数のチケット）55、アクセスチケット検索部56、および証明情報演算部57を持つ。また、カプセル化コンテンツ54には、乱数発生部58、チケット公開鍵法数保持部59、チケット公開鍵保持部60、慣用暗号復号部61、暗号化された慣用鍵の保持部62、および暗号化コンテンツ保持部63を有する。

【0066】次に、ユーザ環境50での処理について述べる。図11および図12にユーザ環境50での処理を示す。ユーザ環境では以下の処理を行う。

【ステップS31】 カプセル化コンテンツ54が乱数 r を生成する。

【ステップS32】 カプセル化コンテンツ54が $r^{E K^E} \bmod n$ を計算し、この値とコンテンツの公開鍵法数 n とをユーザツール53に送付する。 r を用いるのはトークンとの通信路上で慣用暗号鍵を知られるのを防ぐためである。

【ステップS33】 ユーザツール53が、管理しているチケット保持部55から、 n を法数として持つアクセスチケットを全て検索する。チケット保持部55は、法数 n と対応するチケットを組にして保持している。

【ステップS34】 アクセスチケットが1つも見つからない場合は、処理を終了する。

【ステップS35】 検索したチケットの中から、利用制限情報の残り使用回数 U_r が0のチケットで、最も使用順位の値が大きいものを選択する。

【ステップS36】 現在のチケットと同じ法数 n を持つチケットの中から、現在のチケットの次に使用順位の

値が大きいチケットを検索する。

【ステップS37、S38、S39】 チケットが見つかった場合、そのチケットの活性化情報の値を調べ、その値が0の場合には現在のチケットの活性化情報の値を書き込む。そして、 $r^{E K^E} \bmod n$ 、法数 n 、現在のチケットの利用制限情報 L 、及び次のチケットの活性化情報 α の値をトークン52に送る。活性化情報がゼロでない場合はそのまま $r^{E K^E} \bmod n$ 、法数 n 、現在のチケットの利用制限情報 L 、及び次のチケットの活性化情報 α の値をトークン52に送る。

【ステップS36、S40】 チケットが見つからない場合、 α の値を0をとって、 $r^{E K^E} \bmod n$ 、 n 、 L 、 α の組みをトークン52に送る。

【ステップS41】 トークン52が、

【0067】

【数3】 $R1 = (r^{E K^E})^{F(du, L, n)}$

$R2 = (\alpha)^{F(du, L, n)}$

を計算する。

【ステップS42】 ユーザツール53は、トークン52が計算を行っている間に、 $(r^{E K^E})^t$ の値を計算する。

【ステップS43】 トークン52は、計算した $R1$ 、 $R2$ の値をユーザツール53に送る。

【ステップS44～S46】 次の使用順位のチケットがある場合には、ユーザツール53は次のチケットの利用制限情報中の残り回数 U_r の値を1減らし、さらに、次のチケットの活性化情報フィールドの値を、 $R2$ の値で置き換える。

【ステップS47】 トークン52から受け取った $R1$ から、

$(r^{E K^E})^t \cdot R1^{-1} = r^{K^E} \bmod n$

を計算してカプセル化コンテンツ54に送付。

【ステップS48】 カプセル化コンテンツ54は、 r^{K^E} より K を求める。 r の値はカプセル化コンテンツ49が発生させたものなので、 K の計算が可能である。

【ステップS49】 カプセル化コンテンツ54は、 K により暗号化されたコンテンツ本体を慣用暗号復号部61により復号して利用する。

【0068】最初のチケット t_1 を1回使用した時点での、利用制限情報は図13に示すようになる。

【0069】ユーザがコンテンツを利用すると、その利用時点での利用条件がトークン52に履歴として記録される。同じコンテンツであっても利用時点での利用条件での履歴が記録されるため、定まった利用順序・回数で定まった利用条件によるコンテンツの利用が可能になる。

【0070】このようにチケットと利用制限情報の組を計算しておくことにより、例えば、第一のチケット t_1 を特定回数使うことで始めて、 t_2 の計算に用いられた L_2 中の α_2 を計算する事ができ、第二のチケットが利

用可能になる。第2のチケットの利用条件を第1のチケットと異なるものとする事で、例えば利用料金の割引などを行う事が可能になる。同様の処理により、順次異なった条件のチケットを、定まった順序・回数で利用する仕組みが実現できる。

【0071】〔実施例3〕本実施例では特に、1つのコンテンツを特定の回数利用する事により、それとは異なったコンテンツの使用を定められた順番で可能にする方法について述べる。

【0072】本実施例では実施例2と同様にアクセスチケットによる処理を行う。

【0073】本実施例の構成は実施例2と同様であるが、アクセスチケットの利用制限情報に、使用順位の代わりに、次に使用可能となるコンテンツに対応する法数を入れるフィールドが追加される点が異なる。

【0074】実施例の動作について説明する。

【0075】実施例2と同様の方法により、コンテンツプロバイダ40はセンタ30から発行してもらった公開鍵を用いてコンテンツをカプセル化して配布する。ユーザは同様に、センタ30に対してアクセスチケットの発行を要求する。

【0076】ここで、あるコンテンツを特定回数利用した場合のみ、それとは異なるコンテンツを定まった順番で利用できるようにするため、アクセスチケットを発行する際に、センタは以下のように、複数のチケットとそれに対応する利用制限情報を用意する。本実施例では4種類の異なったコンテンツと、それぞれのコンテンツに対応するアクセスチケットとそれに対応する利用制限情報(図14)を用意する。

【0077】アクセスチケットは次式のようなものである。

【0078】

【数4】 $t1 = D1 + F(du, L1, n1)$

$t2 = D2 + F(du, L2, n2)$

$t3 = D3 + F(du, L3, n3)$

$t4 = D4 + F(du, L4, n4)$

利用制限情報は図14に示すようなものである。

【0079】上記の式および図14において式「 $(\alpha 1)^{FUr2(du, L1, n2)} \bmod n$ 」は、 $\alpha 1$ を $F(du, L1, n2)$ で Ur 2回べき乗し、 n に関する剰余をとることを表す。 t はチケット、 D はコンテンツの公開鍵に対応する秘密鍵、 F は方向性関数(例えばMD5などのハッシュ関数)、 du はユーザの秘密鍵、 n はコンテンツの公開鍵法数、 Ur はチケット発行時に生成される乱数、 L は利用条件などを記した利用制限情報である。

【0080】利用制限情報 L は、対応するチケットによるコンテンツの利用に関する情報を記述したもので、アクセスチケットが利用できる期限を示す使用期限や、このチケットによってコンテンツを利用した場合の1回の

利用料金などが記述されている。コンテンツを利用した場合には、この情報に従って課金が行われる。さらに、利用制限情報 L には、次のアクセスチケットを使用可能にするためのチケット活性化情報 α 、次のアクセスチケットが使用可能になるまでの回数 Ur 、および次に使用可能になるチケットの法数が含まれている。

【0081】チケット生成時には、 t は L を上記の表のように設定して計算される。すなわち、 Ur の値を全て0とし、 α の計算にのみ実際の Ur の値が用いられる。

【0082】ユーザには $t1$ から $t4$ の一連のチケットと、利用制限情報 $L1 \sim L4$ を含むアクセスチケットが配布される。但し、ユーザへの配布時には $L1 \sim L4$ は、図15に示すように $Ur1 \sim Ur4$ に値が設定され、さらに $L2 \sim L4$ の $\alpha 2 \sim \alpha 4$ の値を0としたものに置き換えられる。

【0083】次に、ユーザ環境での処理について述べる。ユーザ環境50の構成は実施例2と同様である。図16および図17にユーザ環境50での処理を示す。ユーザ環境50では以下の処理を行う。

〔ステップS51〕 カプセル化コンテンツ54が乱数 r を生成する。

〔ステップS52〕 カプセル化コンテンツ54は $r^K \bmod n$ を計算し、この値とコンテンツの公開鍵法数 n をユーザツール53に送付する。 r を用いるのはトークン52との通信路上で慣用暗号鍵を知られるのを防ぐためである。

〔ステップS53〕 ユーザツール53は、管理しているチケット保持部55から、 n を法数として持つチケットを検索する。チケット保持部55は、法数 n と対応するチケットを組にして保持している。

〔ステップS54〕 チケットが見つからなかった場合は処理を終了する。

〔ステップS55〕 検索したチケットの残り利用回数 Ur が0でなければ、そのチケットはまだ有効ではないので、処理を終了する。

〔ステップS56〕 ユーザツール53は現在のチケットの利用制限情報 L の、次のチケットの法数の値を調べる。

〔ステップS57～S60〕 法数の値が0ではなく、この法数に対応する次のチケットが存在する場合、そのチケットの活性化情報の値を調べ、その値が0の場合には現在のチケットの活性化情報の値を書き込む。

〔ステップS61〕 さらに $r^K \bmod n$ 、法数 n 、現在のチケットの利用制限情報 L 、及び次のチケットの活性化情報 α の値をトークン52に送る。

〔ステップS62〕 次のチケットの法数の値が0か、法数の示すチケットが存在しない場合には、 α の値を0をとって、 $r^K \bmod n$ 、 n 、 L 、 α の組みをトークン52に送る。

〔ステップS63〕 トークン52は

【0084】

【数5】 $R1 = (r^E K^E)^{F(du, L, n)}$ 、

$R2 = (\alpha)^{F(du, L, n)}$

を計算する。

【ステップS64】 ユーザツール53はトークン52が計算を行っている間に、 $(r^E K^E)^t$ の値を計算する。

【ステップS65】 トークン52は、計算したR1、R2の値をユーザツール53に送る。

【ステップS66～S68】 次のチケットがある場合には、ユーザツール53は、次のチケットの利用制限情報中の残り回数Urの値を1減らし、さらに、次のチケットの活性化情報フィールドの値を、R2の値で置き換える。

【ステップS69】 トークン52から受け取ったR1から、

【0085】

【数6】 $(r^E K^E)^t \cdot R1^{-1} = r K \bmod n$ を計算してカプセル化コンテンツ54に送付する。

【ステップS70】 カプセル化コンテンツ54は、rKよりKを求める。rの値はカプセル化コンテンツ54が発生させたものなので、Kの計算が可能である。

【ステップS71】 カプセル化コンテンツ54は、Kにより暗号化されたコンテンツ本体を慣用暗号復号部61により復号して利用する。

【0086】 最初のチケットt1を1回使用した時点での、利用制限情報は図18に示すようになる。

【0087】 実施例2と同様の方法により、ユーザの利用に応じて利用履歴がトークン52に記録され、これをセンタ30が回収する事により、利用者への課金とコンテンツプロバイダ40への料金の分配が行われる。

【0088】 このようにチケットと利用制限情報の組をあらかじめ計算して配布することにより、例えば、第一のチケットt1を特定回数使うことで始めて、t2の計算に用いられたL2中の $\alpha 2$ を計算する事ができ、第二のチケットが利用可能になる。第2のチケットには異なるコンテンツが対応づけられており、これにより、定まった順序で次のコンテンツを使用させる事ができる。同様の処理により、順次異なったコンテンツを、あらかじめ定められた順序でのみ利用させる仕組みが実現できる。

【0089】 また、本実施例の変形として、2つのアクセスチケットを1回ずつ利用する事で、はじめて他のチケットを使用可能にするような仕組みも実現可能である。そのために、センタは以下のようなチケットと利用制限情報を用意する。

【0090】 アクセスチケットは次のようなものである。

【0091】

【数7】 $t1 = D1 + F(du, L1, n1)$

$t2 = D2 + F(du, L2, n2)$

$t3 = D3 + F(du, L3, n3)$

利用制限情報は図19に示すようなものである。

【0092】 上記の式および図19において、Ir1、Ir2はチケット発行時に生成される乱数、Nはこのチケットを活性化させるのに必要な活性化情報の数である。また、fは使用履歴を示すフラグで、1度使われるとこの値は1に書き換えられる。

【0093】 ユーザにはt1からt3の一連のチケットと、利用制限情報L1～L3を含むアクセスチケットが配布される。但し、ユーザへの配布時には図20に示すように、L3は、 $\alpha 3$ の値を0としたものに置き換えられる。

【0094】 t1、t2を最初に使用すると、それぞれの使用履歴が1に書き換えられるとともに、t3のための活性化情報

【0095】

【数8】 $\alpha 1' = \alpha 1^{F(du, L1, n1)}$

$\alpha 2' = \alpha 2^{F(du, L2, n2)}$

が計算されて、L3に保持される。t3を使用する際に、N3個の必要な活性化情報がそろっていた場合には、

【0096】

【数9】 $\alpha 3 = \alpha 1' + \alpha 2' = \alpha 1^{F(du, L1, n1)} + \alpha 2^{F(du, L2, n2)}$

が計算できるので、t3の使用が可能になる。

【0097】 このようにすることで、t1、t2の利用の順番を特定せずに、両方のチケットを使ったときのみ、t3が有効になる仕組みを実現できる。

【0098】

【発明の効果】 以上のように、本発明を用いる事で、オフライン環境下においても、ユーザ環境および提供するコンテンツそのものに特段の機構を追加することなく、また、センタとのコンテンツの利用毎の通信を伴うこともなしに、暗号化されたコンテンツ（あるいは暗号鍵）の利用順序の制御が可能になる。

【図面の簡単な説明】

【図1】 本発明の実施例1の構成を示すブロック図である。

【図2】 実施例1の処理を説明するフローチャートである。

【図3】 実施例1の処理を説明するフローチャートである。

【図4】 実施例1の鍵保持部の構造（初期値）を示す図である。

【図5】 実施例1の鍵保持部の構造（2番目の鍵K2が使用可能になった状態）を示す図である。

【図6】 本発明の実施例2で用いるアクセスチケットによる処理を説明する図である。

【図7】 アクセスチケットの構成を示す図である。

【図 8】 実施例 2 の利用制限情報を説明する図である。

【図 9】 実施例 2 の利用制限情報（ユーザに当初送られるもの）を説明する図である

【図 10】 実施例 2 のユーザ環境の構成を示すブロック図である。

【図 11】 実施例 2 の動作を説明するためのフローチャートである。

【図 12】 実施例 2 の動作を説明するためのフローチャートである。

【図 13】 実施例 2 の利用制限情報（最初のチケットを 1 回利用した後のもの）を説明する図である。

【図 14】 本発明の実施例 3 の利用制限情報を説明する図である。

【図 15】 実施例 3 の利用制限情報（ユーザに当初送られるもの）を説明する図である。

【図 16】 実施例 3 の動作を説明するフローチャート

である。

【図 17】 実施例 3 の動作を説明するフローチャートである。

【図 18】 実施例 3 の利用制限情報（最初のチケットを 1 回利用した後のもの）を説明する図である。

【図 19】 実施例 3 の変形例の利用制限情報を説明する図である。

【図 20】 上述変形例の利用制限情報（ユーザに当初送られるもの）を説明する図である。

10 【符号の説明】

- 10 利用環境（ホスト）
- 11 暗号化コンテンツ保持部
- 12 鍵保持部
- 20 トークン
- 21 鍵活性化情報演算部
- 22 慣用暗号復号部 22

【図 4】

鍵 ID	鍵	次の鍵 ID	鍵活性化情報	使用可能になるまでの回数
I_1	K_1	I_2	0	0
I_2	K_2'	I_3	0	$Ur2$
I_3	K_3'	I_4	0	$Ur3$
I_4	K_4'	0	0	$Ur4$

【図 5】

鍵 ID	鍵	次の鍵 ID	鍵活性化情報	使用可能になるまでの回数
I_1	K_1	I_2	$\alpha_1' = P^{Ur1-1}(\alpha_1)$	0
I_2	$K_2 = K_1 + P(\alpha_1')$	I_3	0	0
I_3	K_3'	I_4	0	$Ur3$
I_4	K_4'	0	0	$Ur4$

【図 7】

アクセスチケット
チケット法数 n
公開鍵 E
チケット本体 t
利用制限情報 L

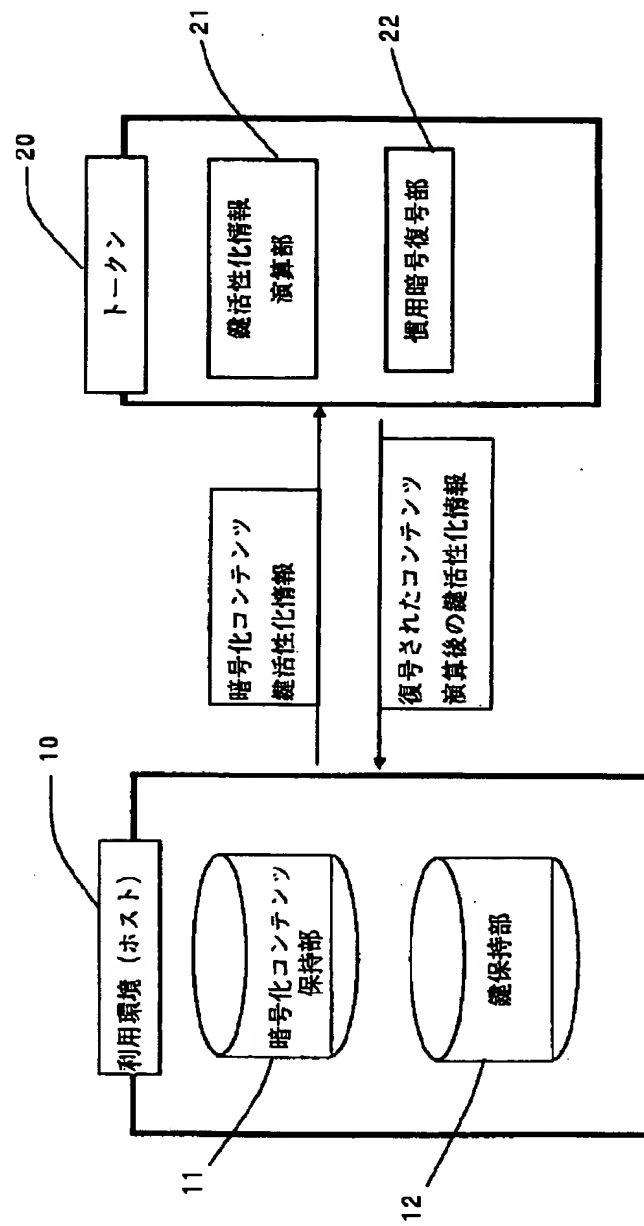
【図 9】

利用制限情報	使用期限	利用料金	使用順位	使用可能になるまでの回数	チケット活性化情報
L_1	1997/12/31	100	1	$Ur1=0$	$\alpha_1 = Ir$
L_2	1997/12/31	80	2	$Ur2=20$	$\alpha_2 = 0$
L_3	1997/12/31	60	3	$Ur3=20$	$\alpha_3 = 0$
L_4	1997/12/31	40	4	$Ur4=20$	$\alpha_4 = 0$

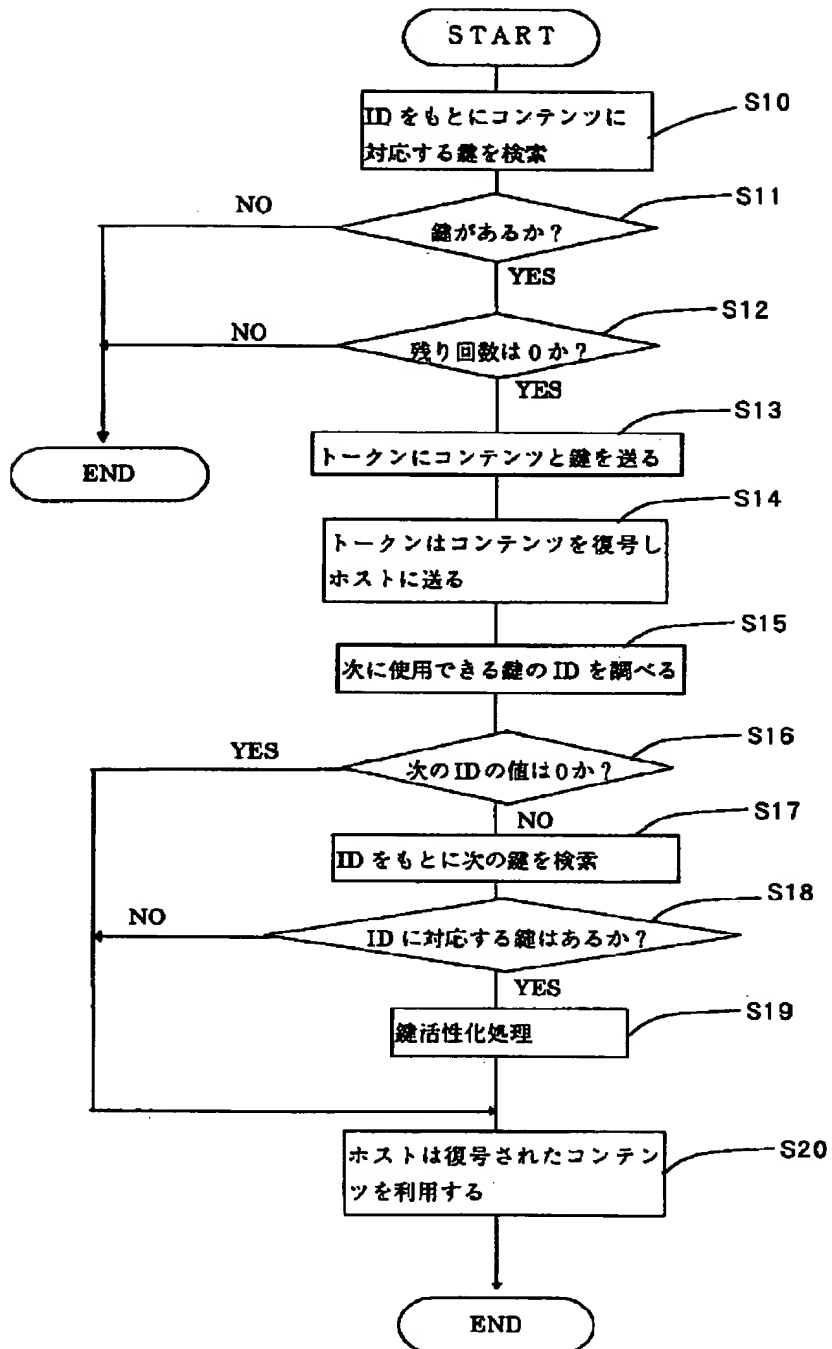
【図 13】

利用制限情報	使用期限	利用料金	使用順位	使用可能になるまでの回数	チケット活性化情報
L_1	1997/12/31	100	1	$Ur1=0$	$\alpha_1 = Ir$
L_2	1997/12/31	80	2	$Ur2=19$	$\alpha_2 = (\alpha_1)^{P^{Ur1-L_2}} \bmod n$
L_3	1997/12/31	60	3	$Ur3=20$	$\alpha_3 = 0$
L_4	1997/12/31	40	4	$Ur4=20$	$\alpha_4 = 0$

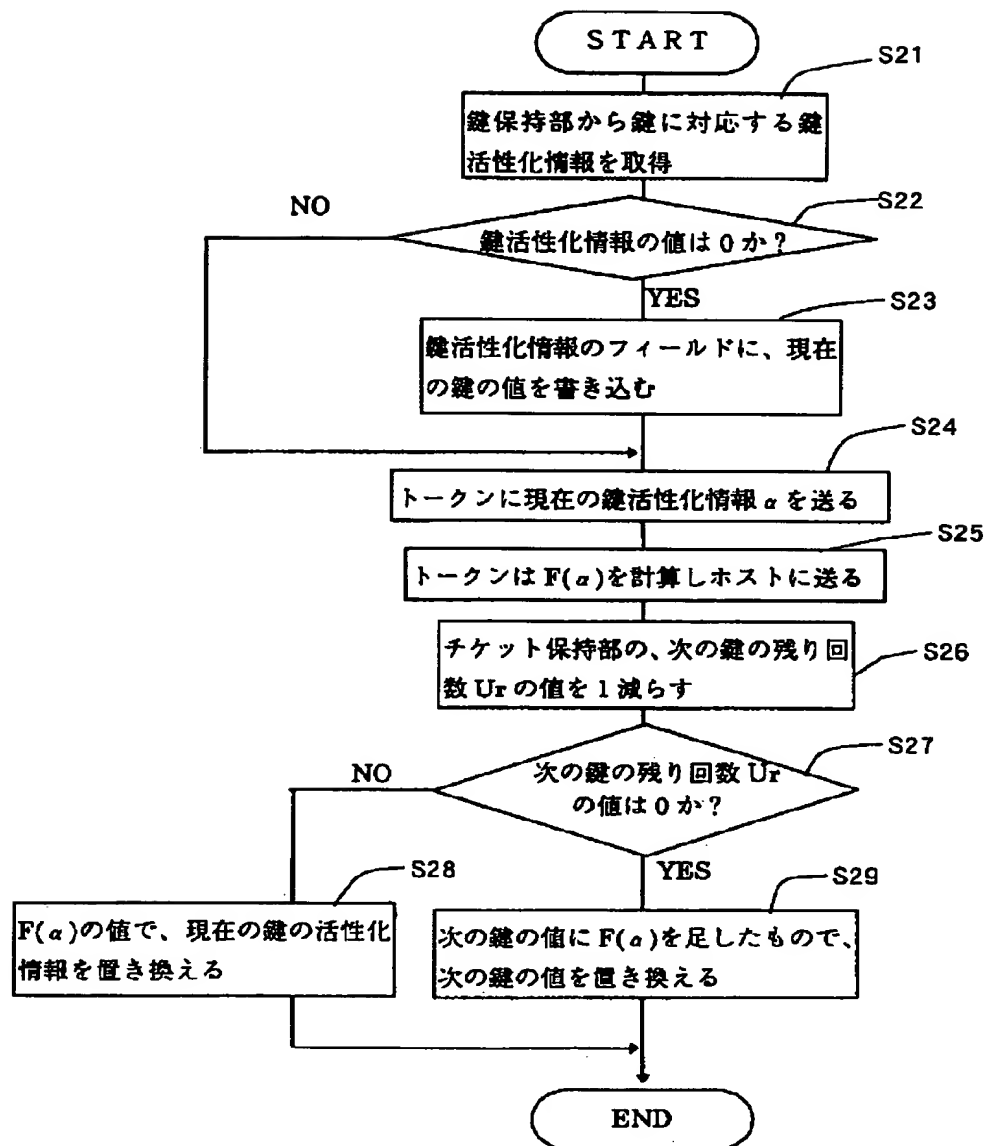
【図1】



【図2】



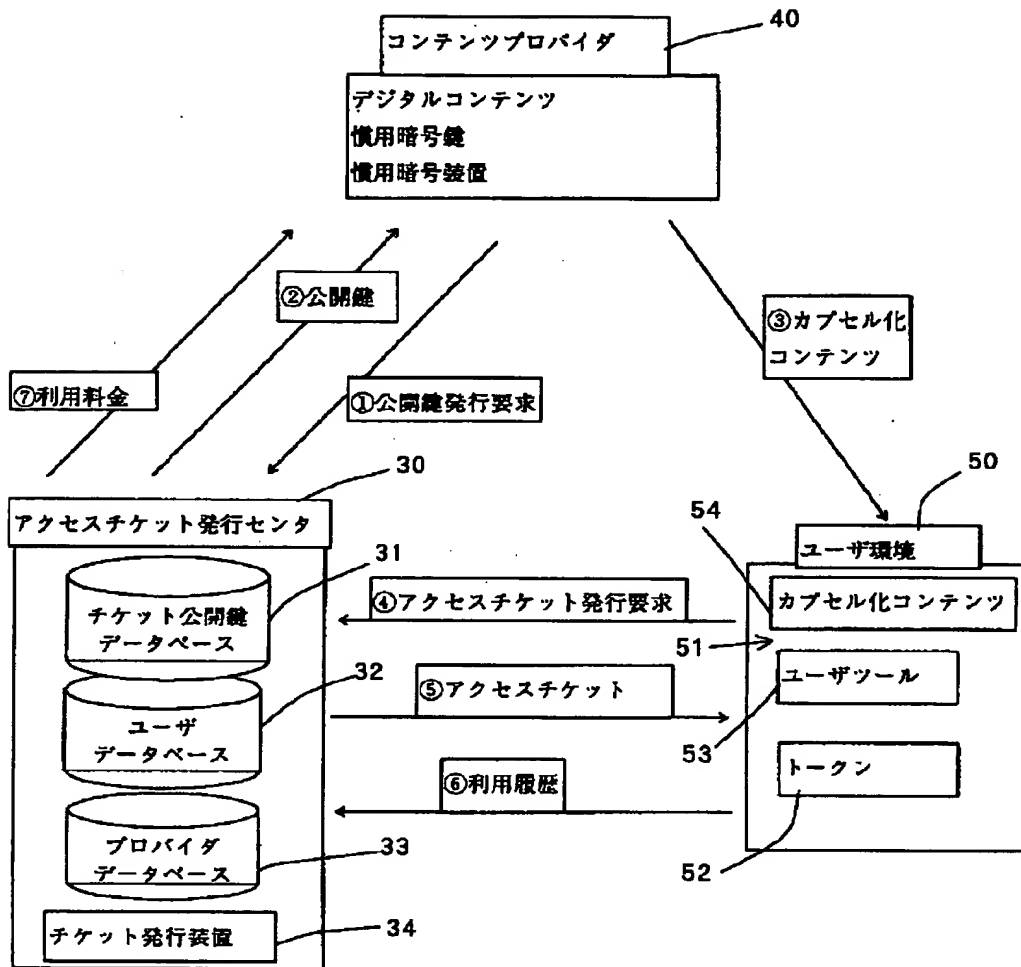
【図3】



【図19】

利用制限情報	使用期限	利用料金	次のチケットの注数	使用履歴を示すフラグ	必要な活性化情報の数	チケット活性化情報 α
L_1	1997/12/31	100	N_1	0	$N_1=1$	$\alpha_1 = I_{r1}$
L_2	1997/12/31	100	N_2	0	$N_2=1$	$\alpha_2 = I_{r2}$
L_3	1997/12/31	100	0	0	$N_3=2$	$\alpha_3 = \alpha_1(F(\alpha_2, I_{r3})) + \alpha_2(F(\alpha_1, I_{r3}))$

【図6】



【図14】

利用制限情報	使用期限	利用 料金	次のチケットの 法数	使用可能になる までの回数 U_r	チケット活性化情報 α
L_1	1997/12/31	100	n_1	$U_{r1}=0$	$\alpha_1=1r$
L_2	1997/12/31	100	n_2	$U_{r2}=0$	$\alpha_2 = (\alpha_1)^{P^{U_{r1}}(n_1, L_1, n_2) \bmod n}$: $U_{r2}=20$
L_3	1997/12/31	100	n_3	$U_{r3}=0$	$\alpha_3 = (\alpha_2)^{P^{U_{r2}}(n_2, L_2, n_3) \bmod n}$: $U_{r3}=20$
L_4	1997/12/31	100	0	$U_{r4}=0$	$\alpha_4 = (\alpha_3)^{P^{U_{r3}}(n_3, L_3, n_4) \bmod n}$: $U_{r4}=20$

【図8】

利用制限情報	使用期限	利用料金	使用 順位	使用可能になる までの回数 U_r	チケット活性化情報 α
L_1	1997/12/31	100	1	$U_{r1}=0$	$\alpha_1=I_r$
L_2	1997/12/31	80	2	$U_{r2}=0$	$\alpha_2=(\alpha_1)^{F_{U_{r2}}(du,L_1,n)} \bmod n$: $U_{r2}=20$
L_3	1997/12/31	60	3	$U_{r3}=0$	$\alpha_3=(\alpha_2)^{F_{U_{r3}}(du,L_2,n)} \bmod n$: $U_{r3}=20$
L_4	1997/12/31	40	4	$U_{r4}=0$	$\alpha_4=(\alpha_3)^{F_{U_{r4}}(du,L_3,n)} \bmod n$: $U_{r4}=20$

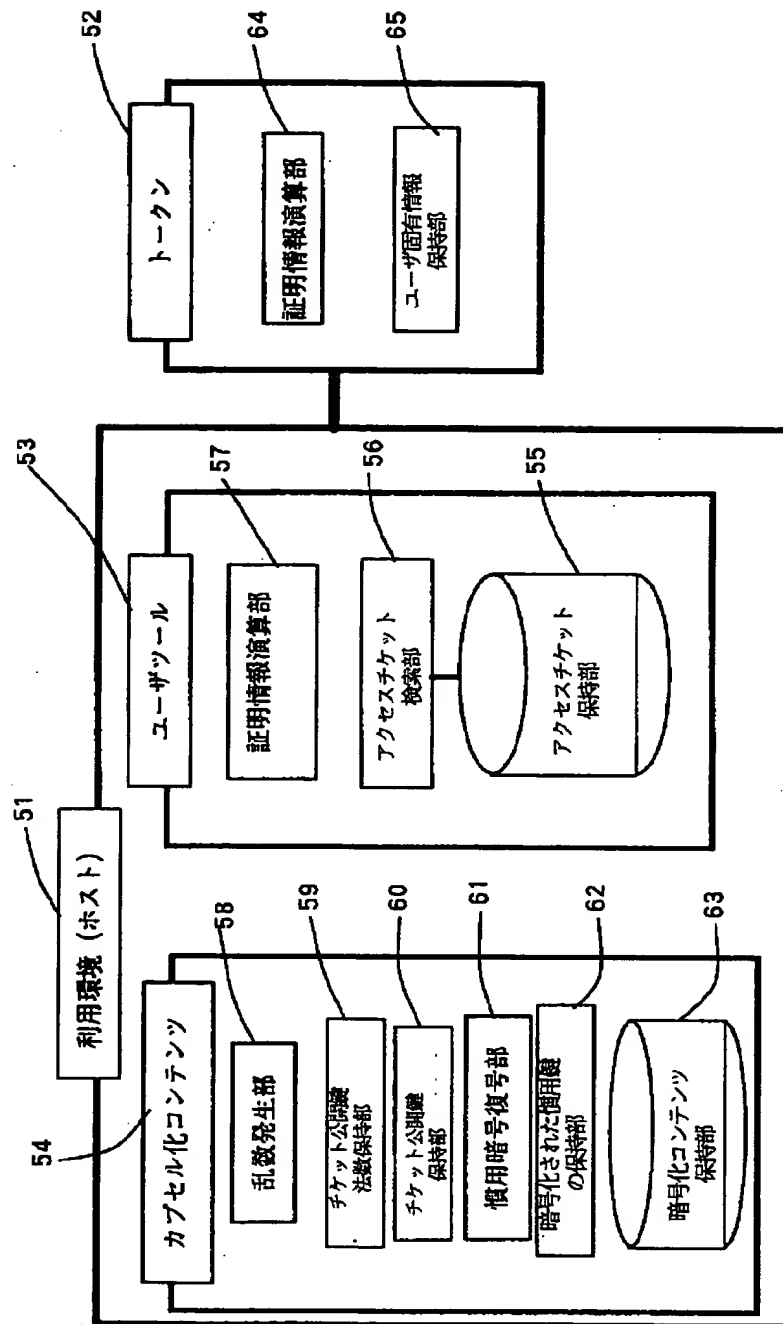
【図15】

利用制限情報	使用期限	利用料金	次のチケットの法数	使用可能になる までの回数	チケット活性化情報
L_1	1997/12/31	100	m_1	$U_{r1}=0$	$\alpha_1=I_r$
L_2	1997/12/31	100	m_2	$U_{r2}=20$	$\alpha_2=0$
L_3	1997/12/31	100	m_3	$U_{r3}=20$	$\alpha_3=0$
L_4	1997/12/31	100	0	$U_{r4}=20$	$\alpha_4=0$

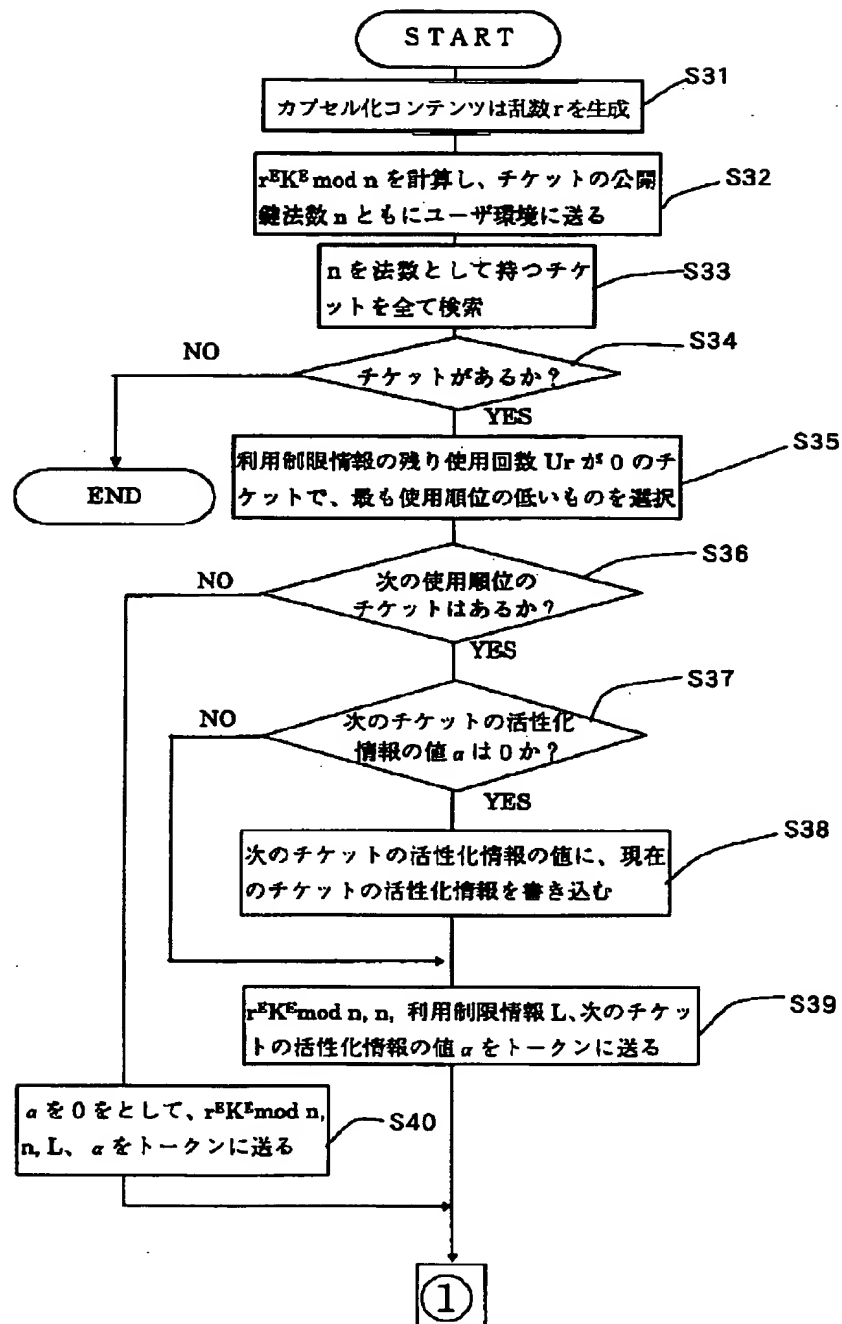
【図20】

利用制限 情報	使用期限	利用 料金	次のチケットの法数	使用期限を 示すフラグ f	必要な活性化 情報の数	チケット活性化情報 α
L_1	1997/12/31	100	m_1	0	$N_1=1$	$\alpha_1=I_{r1}$
L_2	1997/12/31	100	m_2	0	$N_2=1$	$\alpha_2=I_{r2}$
L_3	1997/12/31	100	0	0	$N_3=2$	$\alpha_3=0$

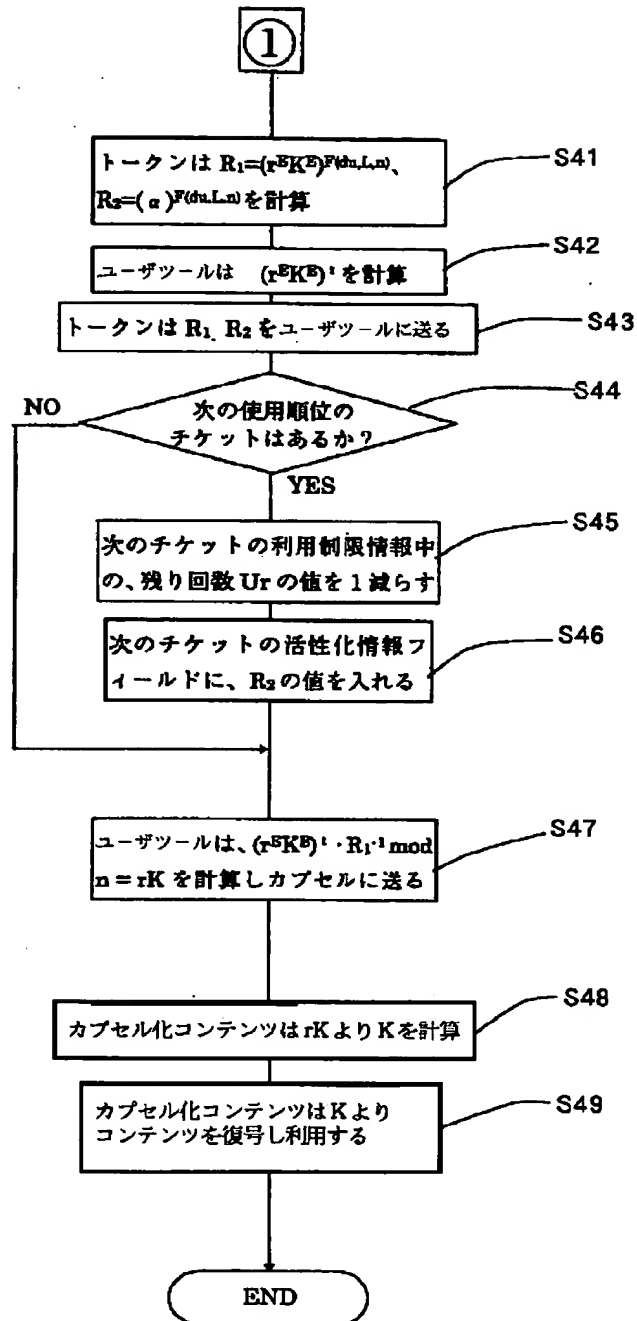
【図10】



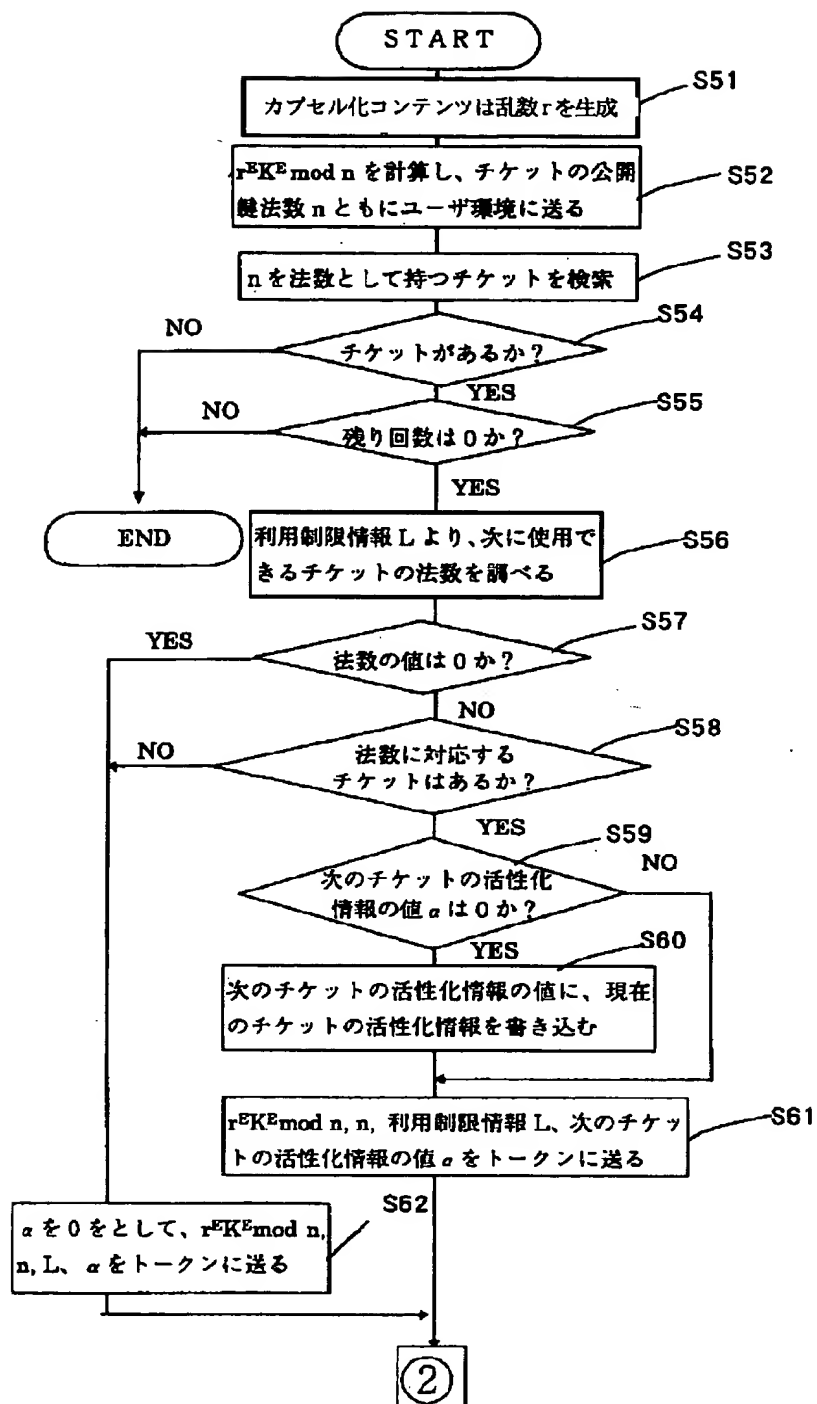
【図11】



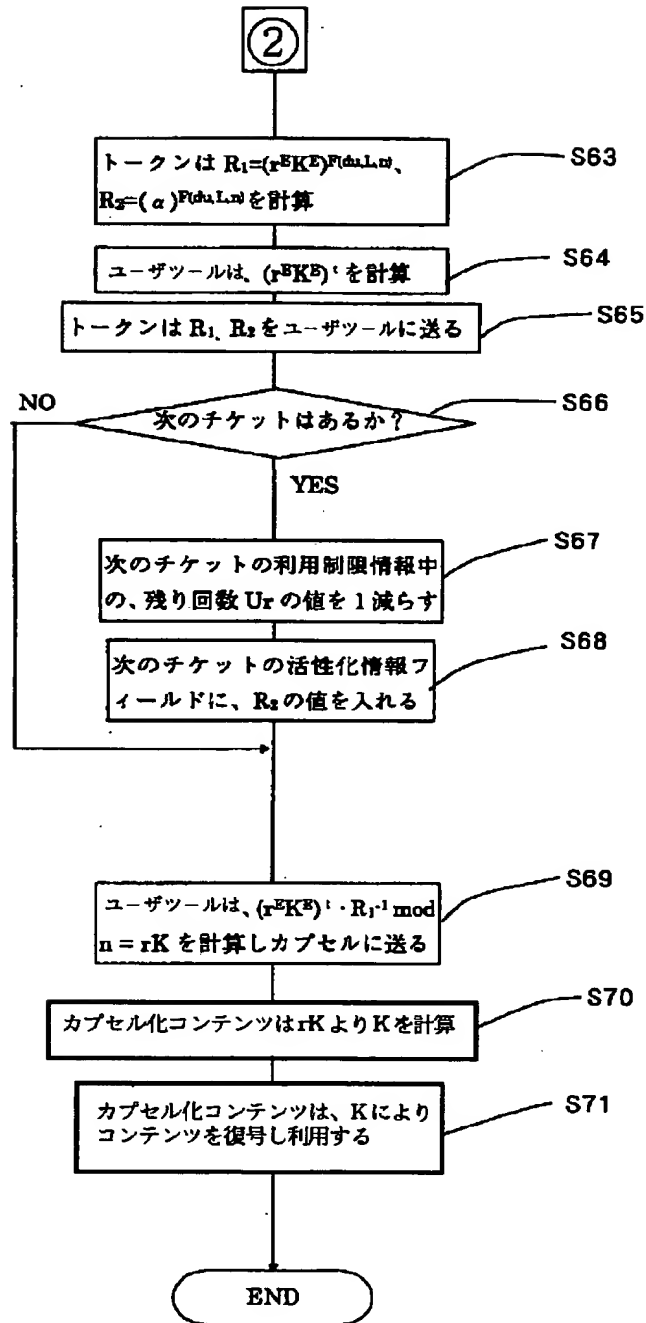
【図12】



【図16】



【図17】



【図18】

利用制取情報	使用期限	利用料金	次のチケットの法数	使用可能になるまでの回数	チケット活性化情報
L_1	1997/12/31	100	m	$Ur1=0$	$e_1=Ir$
L_2	1997/12/31	100	m	$Ur2=19$	$e_2=(e_1)^{P_{m-1}+1} \bmod n$
L_3	1997/12/31	100	m	$Ur3=20$	$e_3=0$
L_4	1997/12/31	100	0	$Ur4=20$	$e_4=0$

フロントページの続き

(51) Int. Cl.⁶

// G 0 6 F 12/14

識別記号

3 2 0

F I

H 0 4 L 9/00

6 0 1 E

6 4 1